## CLAIMS

What is claimed is:

1. A data storage security system, comprising:

at least one hierarchical data structure associated with one or more data items; and

a security component that applies at least one security policy to the data items from a global location associated with a data store.

2. The system of claim 1, the hierarchical data structure is at least one of a tree structure and a containment hierarchy.

3. The system of claim 2, the containment hierarchy is modeled as a Directed Acyclic Graph (DAG).

4. The system of claim 1, the security policy is mapped to one or more security regions that are associated with the database.

5. The system of claim 4, the security policy is at least one of mapped from within the database and mapped from outside the data store.

6. The system of claim 1, the security policy is at least one of explicitly mapped to an item and inherited by an item.

7. The system of claim 1, the security component includes an Access Control List having one or more Access Control Entries.

8. The system of claim 7, the Access Control List can be associated with a holding relationship of a containment hierarchy.

9. The system of claim 8, further comprising a plurality of Access Control Lists to facilitate security for the containment hierarchy.

10. The system of claim 1, the security component specifies a set of principals that are granted or denied access to perform operations on an item.

11. The system of claim 1, the security component includes at least one of discretionary access control list, a system access control list, and a security identifier.

12. The system of claim 1, further comprising an ordering component that arranges one or more Access Control Entries (ACE) in an Access Control List (ACL) to determine a security policy that is enforced for an item.

13. The system of claim 12, further comprising the following ordering algorithm:

For inherited ACL's (L) on item (I)

For items I1, I2

For ACE's A1 and A2 in L,

I1 is an ancestor of I2 and

I2 is an ancestor of I3 and

A1 is an ACE inherited from I1 and

A2 is an ACE inherited from I2

Implies

A2 precedes A1 in L,

wherein L and I are integers.

14. The system of claim 12, further comprising the following ordering algorithm:

For inherited ACL's (L) on item (I)

For items I1

For ACE's A1 and A2 in L,

I1 is an ancestor of I2 and

A1 is an ACCESS_DENIED_ACE inherited from I1 and

A2 is an ACCESS_GRANTED_ACE inherited from I1

Implies

A1 precedes A2 in L,

wherein L and I are integers.

15. The system of claim 12, further comprising a component that evaluates access rights for a given principal to a given item.

16. The system of claim 1, the security component further comprises an effective access control list that is obtained by processing lists inherited by an item and adding inheritable access control entries in an explicit access control list.

17. The system of claim 1, the security component further comprises an access mask specifying at least one of object-specific access rights, standard access rights, and generic access rights.

18. The system of claim 1, further comprising a security table for similarly protected security regions.

19. The system of claim 18, the security table includes at least one of the following fields an Item Identity, an Item Ordpath, an Explicit Item, a Path ACL, and a Region ACL.

20. The system of claim 1, further comprising a component to at least one of create a new item in a container, add an explicit ACL to an item, add a holding link to an item, delete a holding link from an item, delete an explicit ACL from an item and modify an ACL associated with an item.

21. A computer readable medium having computer readable instructions stored thereon for implementing the security component of claim 1.

22. A method to facilitate data item security, comprising:
defining at least one security policy for a hierarchical data structure;
defining at least one security region for the hierarchical data structure; and
applying the security policy to the hierarchical data structure from the security region.

23. The method of claim 22, further comprising automatically supporting at least one explicit and inherited security policy.

24. The method of claim 22, further comprising automatically ordering security policies.

25. The method of claim 22, further comprising processing security policies for at least one of a tree structure and a containment hierarchy.

26. The method of claim 22, further comprising mapping a security policy to a security region from a remote location from a database.

27. The method of claim 22, the security policy is associated with an Access Control List having one or more Access Control Entries.

28. The method of claim 27, further comprising automatically arranging one or more Access Control Entries in the Access Control List to determine a security policy that is enforced for an item.

29. A system to facilitate database security processing, comprising:

means for defining a security policy;

means for determining a security region for the security policy; and

means for applying the security policy to at least one of a tree structure and a containment hierarchy in accordance with the security region.

30. A computer readable medium having a data structure stored thereon, comprising:

a first data field related to a security region associated with a hierarchical data structure;

a second data field that relates to a security policy; and

a third data field that links the security policy to the security region.

31. The computer readable medium of claim 30, further comprising a field for an access mask specifying at least one of object-specific access rights, standard access rights, and generic access rights.

32. The computer readable medium of claim 30, further comprising a security field for similarly protected security regions.

33. The computer readable medium of claim 32, the security table field includes at least one of an Item Identity, an Item Ordpath, an Explicit Item, a Path ACL, and a Region ACL.